ICS 35.030
CCS L 80

# 中华人民共和国密码行业标准

GM/T 0033—2023
代替 GM/T 0033—2014

# 时间戳接口规范

**Interface specifications of time stamp**

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0033—2014《时间戳接口规范》，与GM/T 0033—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了规范性引用文件GM/T 0028（见7.1）、GM/T 0081（见7.2）、GM/Z 4001（见第3章）、RFC 5035（见7.1）、RFC 6211（见7.1），删除了规范性引用文件GM/T 0006（见2014年版的5.1）、RFC 3066（见2014年版的7.2），将规范性引用文件GM/T 0010更改为GB/T 35275（见7.1，2014年版的7.2），将规范性引用文件RFC 3369更改为GB/T 31503（见7.2，2014年版的7.2）；

b) 删除了术语“证书认证机构”（见2014年版的3.1）、“密码杂凑算法”（见2014年版的3.2）、“数字签名”（见2014年版的3.3）、“SM2算法”（见2014年版的3.4）、“时间戳”（见2014年版的3.5）、“时间戳系统”（见2014年版的3.6）；

c) 增加了缩略语“TSA”“HTTPS”（见第4章，2014年版的第4章）；

d) 更改了图1（见6.1，2014年版的6.1）；

e) 更改了时间戳请求格式中有关杂凑算法标识的定义，增加了时间戳响应中对算法保护域的要求（见7.1、7.2，2014年版的7.1、7.2）；

f) 更改了8.4的名称，由“HTTP方式”改为“HTTPS/HTTP方式”（见8.4，2014年版的8.4）；

g) 增加了“获取时间戳响应状态信息”函数STF_GetTSStatus（见9.6）；

h) 更改了STF_CreateTSRequest、STF_CreateTSResponse和STF_VerifyTSValidity的参数，用以支持更多的时间戳请求的属性（见9.4、9.5、9.7，2014年版的9.4、9.5、9.6）；

i) 增加了时间戳接口错误代码STF_TS_ITEM_NOT_EXIST的定义（见附录A）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：上海市数字证书认证中心有限公司、北京数字认证股份有限公司、格尔软件股份有限公司、长春吉大正元信息技术股份有限公司、北京海泰方圆科技股份有限公司、无锡江南信息安全工程技术中心、中电科网络安全科技股份有限公司、兴唐通信科技有限公司、上海颐东网络信息有限公司、万达信息股份有限公司、飞天诚信科技股份有限公司、北京华大智宝电子系统有限公司、北京握奇智能科技有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心、国家密码管理局商用密码检测中心、三未信安科技股份有限公司。

本文件主要起草人：刘平、刘承、崔久强、李述胜、谭武征、赵丽丽、柳增寿、徐强、李元正、王妮娜、夏东山、李海杰、于华章、陈跃、胡俊义、孔凡玉、袁峰、李志伟、冯晔、王玉林、掌晓愚、李沁芸、郝波、许永欣、王腾飞、胡伯良、李国友、顾伟平。

本文件及其所代替文件的历次版本发布情况为：

——2014年首次发布为GM/T 0033—2014；

——本次为第一次修订。

# 时间戳接口规范

## 1 范围

本文件规定了时间戳服务接口的请求和响应消息的格式、传输方式和时间戳服务接口函数。

本文件适用于基于公钥密码应用技术体系框架内的时间戳服务相关产品的研制。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 31503 信息安全技术 电子文档加密与签名消息语法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GM/T 0019 通用密码服务接口规范

GM/T 0028 密码模块安全技术要求

GM/T 0081 SM9 密码算法加密签名消息语法规范

GM/Z 4001 密码术语

RFC 3161 Internet X.509 公钥基础设施时间戳协议(TSP)[Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)]

RFC 5035 增强安全服务(ESS)更新：增加 CertID 算法灵活性[Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility]

RFC 6211 加密消息语法(CMS)算法标识符保护属性[Cryptographic Message Syntax (CMS) Algorithm Identifier Protection Attribute]

## 3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

**时间戳服务 time stamp service**

时间戳系统给用户提供的颁发时间戳的服务。

注：由用户提供文件，时间戳系统给此文件签发时间戳。

## 4 缩略语

下列缩略语适用于本文件。

DER 可区分编码规则(Distinguished Encoding Rules)

HTTP 超文本传输协议(HyperText Transfer Protocol)

HTTPS 基于安全套接层的超文本传输协议(HyperText Transfer Protocol over Secure Sockets